Integrated Computer and Information Security Training (COM100)

Before you begin your training, remember . . .

You are responsible for:

- protecting information and passwords they control,
- avoiding waste, fraud, or abuse of information resources,
- using only authorized software,
- appropriately marking and handling all print material and media,
- observing information security requirements,
- reporting information security incidents, and
- obeying SNL/DOE information security policies.

Module 1
Unclassified Territory: Who Does What, Where, and Why?

After completing this module, you will be able to:

- recognize the importance of protecting Sandia information,
- identify who's responsible for the information you process,
- distinguish between the two types of unclassified information, and
- distinguish between the two unclassified computing networks.

WHAT IS A RECORD AND WHY PROTECT IT?

Most information used in the course of doing Sandia business is a record, and could result in various degrees of damage to our national security if that information became generally known.

Records come in many different formats. Regardless of media, the same principles apply. Most Sandia records are government property, and are subject to government regulations.

If you have recorded information which documents Sandia or government policies, decisions, procedures, operations, programs, projects, or activities, you are responsible for protecting this information properly.

"Most information used for Sandia business is a record and requires some degree of protection."

TYPES OF UNCLASSIFIED INFORMATION

Before you are authorized to access or process any type of information, its sensitivity level must be determined.

When combining two messages or documents, be aware that this action may require the information to be reclassified.

Sandia's unclassified information is made up of:

- Unclassified Controlled Information, and
- Unclassified Unlimited Release.

"Before you start, know what type of information you are working with."

Unclassified Controlled Information (UCI)

Unclassified Controlled Information:

- was formerly known as UCAI, and
- is commonly known as Sensitive Unclassified.

Protection of this information:

- requires access restrictions and controls,
- is mandated by law, formal agreement, or corporate process requirements (CPRs),
- prevents loss or compromise of Sandia's assets, and
- reduces liabilities for Sandia and the government.

"You're responsible for protecting and managing all information that is part of your work assignment!"

Unclassified Unlimited Release (UUR)

Unclassified Unlimited Release (UUR) requires the least amount of protection.

Protection of this information is NOT mandated by regulation; management of this information is just good business practice.

Unclassified Unlimited Release Information may be:

- made available to the general public,
- left unattended, and
- accessible to anyone (e.g., foreign nationals, student interns, visitors, reporters).

"If you declare your information to be UUR, you still need to manage it!"

Who determines which information is UCI?

- **DOE, federal law, or other federal agencies** may require that controls be placed on the availability of certain information.

- **The information owner** may state that certain information is a type of UCI and protection is required.

Additional protection may be needed because the misuse, alteration, disclosure, or destruction of the information could adversely impact National or DOE interests.

"If you're unsure about what type of information you're working with, ask your manager!"

UNCLASSIFIED COMPUTING NETWORKS

"You need to know which network your computer is connected to, because each network has specific rules to follow."

There are two unclassified networks at SNL:

- the Sandia Restricted Network (SRN), and
- the Sandia Open Network (SON).

Each network has specific rules to follow.

In the Sandia Restricted Network (SRN), you may process:

- Unclassified Controlled Information (UCI), and
- Unclassified Unlimited Release (UUR).

In the Sandia Open Network (SON), you may:

- connect with NON-Sandia organizations, and
- process Unclassified Unlimited Release (UUR).

Users who do NOT have clearances (who are uncleared badged) may be authorized by SNL management to access systems within the SRN or the SON networks.

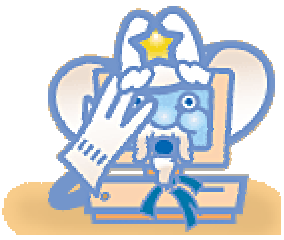
Sandia Restricted Network (SRN)

The purpose of the SRN is to restrict access to information by protecting it behind a firewall.

Specific SRN rules:

- Minimum Desktop Protection requirements must be met.
- Foreign Nationals who have Permanent Resident Alien status can have access.
- Protected dial-up access (e.g. SecurID cards) is allowed.
- Both Unclassified Unlimited Release (UUR) and Unclassified Controlled Information (UCI) are allowed.
- Additional protections are required when processing UCI.
- Protected connections are allowed to other sites (including nation-wide networks).

Sandia Open Network (SON)



"NEVER process UCI on the SON unless it's behind a firewall!"

Specific SON rules:

- All Foreign Nationals are allowed access.
- Minimum Desktop Protection requirements must be met.
- ONLY Unclassified Unlimited Release (UUR) is allowed.
- Non-secure connections to other sites are allowed (including nation-wide networks).

No UCI may be processed on the SON unless it is behind an organization's own firewall (e.g. Computer Science Institute, Robotics Manufacturing and Engineering Lab).

"A computer must NEVER be connected to both the SRN and the SON at the same time."

Connected to each primary network (SRN, SON) are Local Area Networks (LANs), and individual computers are connected to these LANs. A computer not directly connected to one of the primary networks must still abide by the rules of one of the networks.

Module 1: Practice Scenario

Scenario
You have been assigned a project that involves gathering information from several resources. As you gather information and begin to combine it into a document, you wonder whether the data is now sensitive. Your computer is connected to the Sandia Open Network (SON).

1. Where do you go with questions about the type of information you are working with?

    (A) Your manager.

    (B) Records Management Manual.

    (C) Technical Library.

    (D) Document Control Custodian.

2. If the information is determined to be sensitive, in which category does it belong?

    (A) Unclassified Secure Information.

    (B) Unclassified Sensitive Release.

    (C) Unclassified Unlimited Release.

    (D) Unclassified Controlled Information.

3. If the information is determined to be sensitive, where can it be processed

    (A) The Sandia Open Network.

    (B) The Sandia Restricted Network.

    (C) Any Sandia network.

    (D) Any CSU network.

Module 2
Minimum Protections: What Every Law-Abiding Information User Needs to Know

At the end of this module, you will be able to identify:

- minimum desktop protections, and
- minimum information protections.

MINIMUM Desktop Protection

When processing information on a computer, regardless of its sensitivity level, you must meet minimum desktop protections:

- adequate physical security,
- power-on password,
- password protected screen saver/screen lock, and a
- virus scanner.

Any exceptions to the above must be noted in your Center Information Plan and approved before beginning operation of your workstation.

Physical Security

Information can be protected by physical barriers and individual actions.

"Know which type of area you are working in!"

The most common types of security areas within Sandia National Labs are:

- Exclusion Areas,
- Limited Areas, and
- Property Protection Areas.

Each security area provides different degrees of physical protection.

Physical location is just one level of protection. There are also several actions you can take to protect information from damage or loss.

While working with Unclassified Controlled Information (UCI):

position your monitor or work so only people with the need-to-know can see the information, and use a tent card or cover sheet to alert those around you about the sensitivity of the data you're processing.

Before leaving your workspace unattended, at any time:

- activate the password protected screen saver or lock your workstation, and
- protect UCI (documents and removable electronic media) according to the rules for your area.

"NEVER leave your workspace without activating your screensaver and protecting Sandia's information."

A combination of physical barriers and individual actions provide one level of protection for your information. Another level of protection for computers is provided through the use of passwords.

At a minimum, every system must have a password protected screen saver. Outside of the Limited Area every system must also have a power on password.

PASSWORD REQUIREMENTS

All passwords must be machine-generated. Use the Kerberos Password Utility to select a password.

Once you have entered a password, don't leave your system unattended. Anyone sitting at your computer has all of the access granted by your password. To protect your system when unattended, use a password protected screen saver or log off the system.

" Every system must have a password protected screen saver; use your Kerberos password whenever possible."

Your Kerberos password is used to access your timecard, benefits and other secure applications. To protect against unauthorized access to these applications, exit your browser completely after each use of your Kerberos password.

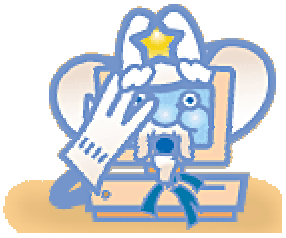
"Protect all passwords."

All unclassified passwords are considered to be Official Use Only, a category of Unclassified Controlled Information (UCI).

You may carry it in your wallet or purse, or you may store it in a locked cabinet or desk. Don't share your passwords with anyone, and don't store passwords on your computer. Any exceptions must be documented in your Center Information Plan.

"Don't give your password to anyone, not even an auditor or CCHD personnel!"

"You must change unclassified passwords annually. If your password is disclosed, change it immediately."



VIRUS CHECKING

Sandia requires that all PC and Macintosh systems use anti-virus software to protect against the loss of information. Sandia makes site-licensed anti-virus software available because recovery costs from virus infections is expensive.

Anti-virus software protects systems by:

- scanning,
- detecting, and
- repairing.

"Prevention is the key! Scan for viruses before you download, copy, or install files or software."

NETWORK INFORMATION SYSTEM

You MUST ensure that your system (networked or standalone) is registered in the Network Information System (NWIS).

Sandia National Laboratories requires that the NWIS database be the primary source for locating all computer systems.

All systems registered in NWIS must display the SNL computer banner or a paper copy of the document next to the computer.

"You MUST verify that ALL your computer systems are registered in NWIS and display the SNL computer banner."

MINIMUM INFORMATION PROTECTION

"YOU'RE responsible for protecting information under your control from being copied, altered, misused, or destroyed."

Regardless of the sensitivity of the information you process, you are responsible for protecting the information under your control - no matter what media it's recorded on.

You accomplish this through:

- files management, and
- records retention.

Files management is the application of records management principles and techniques.

Information can be easily accessed and retrieved if it is arranged in a logical and orderly manner. Files management applies to electronic records as well as to paper and other media.

Records Retention and Disposition Schedule

In order to manage and retain your records efficiently, become familiar with the Sandia Records Retention and Disposition Schedule.

The Sandia Records Retention and Disposition Schedule contains information about groups of records at Sandia.

Use this schedule to determine your records:

- retention period (how long to keep recorded information), and
- office of record (who is responsible for records maintenance).

Module 2: Practice Scenario

Scenario

You have just received a new computer and will be using it to work on an Unclassified Controlled Information project for the next year. You open an e-mail attachment and your anti-virus software notifies you that the attachment contains a virus. You also have been notified to get a new password.

1. In order to protect the information on your new computer, what do you need to verify?

   (A) Warranty registration.

   (B) Both C & D.

   (C) Registration in NWIS.

   (D) SNL computer banner display.

2. Who is responsible for protecting the project information under your control?

   (A) Your manager.

   (B) Your director.

   (C) Your Computer Support Unit.

   (D) You.

3. What actions do you need to take to protect your UCI project information?

   (A) In this case, no actions are necessary.

   (B) Position your monitor or work, set up a tent card, or use a cover sheet.

   (C) Back up the information to a disk, and leave it in the computer.

   (D) Leave the information visible in your workspace.

4. What action must be taken before you leave your workspace unattended?

   (A) Turn your monitor off.

   (B) Activate your password-protected screensaver.

   (C) Both B & D.

   (D) Protect your UCI records.

5. How do you protect your new password?

   (A) Hide it under your keyboard.

   (B) Put it in a locked drawer.

   (C) Hide it in a file folder.

   (D) Store it on SDSS.

Module 3
Basic Protection: When You Move It, Don't Lose It!

At the end of this module, you will be able to identify methods for:

- backing up and recovering computer information,
- receiving and transmitting information via computers,
- transferring computer information that needs to be retained, and
- disposing of recorded information, computer hardware, and media.

INFORMATION BACKUP AND RECOVERY

YOU are responsible for providing for the restoration of systems and recovery of the information you are processing.

Accidents do happen. Ask yourself: "How much can I afford to lose? What resources would it take to recover? How would this loss affect my, or Sandia's, reputation?"

Backup copies of all information are essential to recovery, so you need to back up your information regularly.

" Make sure your information is backed up so you don't lose it - you're responsible for its recovery!"

It is good business practice to store your original information in a separate location from your backups. The Sandia Data Storage Service (SDSS) is located on a corporate server and is available for you to use to back up your information.

Sandia's Blue Label Computer Record Protection Program may also be used to store your back-up media in off-site storage.

Standard recovery methods are to:

- repair damaged systems or replace with new equipment;
- reload operating system and software from master copies;
- recover information from backups;

- periodically test backup systems and disks to ensure they are usable.

RECEIVING & TRANSMITTING INFORMATION VIA COMPUTERS

"Our firewalls are essential to the protection of Sandia information."

Firewall Protection

A firewall is a separation between the unclassified environment and the outside world that allows controlled access to resources.

The purpose of firewall protection is to:

- prevent unauthorized external access to computer files,
- monitor transfers of information to and from networks, and
- block programs which could potentially compromise the security of our networks.

When connecting to an external site, there will be times when you are unable to receive information because of the firewall. Sandia does NOT allow general access to its secure web sites without prior approval.

Communication Devices

"Communication devices" is a term used to describe automated methods for transmitting information from one computer system to another. Numerous computer manufacturers are now shipping computer systems with attachable or built-in communication devices.

When connecting communication devices to your SNL computer, consider corporate rules regarding the:

- type of information you process,
- location of your equipment, and
- your computing environment.
-

"Do NOT connect communication devices without knowing the rules."

You could reveal all information on your machine, as well as on any systems your machine has access to, if communication devices are connected incorrectly.

Modems offer potential pathways for an intruder to enter our networks, so their use must be controlled. If you operate a modem that is EVER connected to the Sandia telephone exchange, you MUST register the phone line (number) using the online registration application.

DISPOSING OF RECORDED INFORMATION

Prior to disposing of ANY recorded information, you must check the:

- **Sandia Records Retention and Disposition Schedule**
  This schedule provides approved disposal dates.

- **Unclassified Controlled Information CPR**
  This CPR provides approved disposal methods by UCI category.

Disposing of Paper & Photo Materials

To dispose of Unclassified Controlled Information (UCI) paper and photos you must:

- shred prior to placing in the trash, or
- place in white burn bag (NM), or UCI mailbox (CA).

You must place UCI negatives or film in a separate container from photos.

You should never dispose of UCI by using any recycle procedure.

To dispose of Unclassified Unlimited Release (UUR) paper and photo materials, you may place:

- white paper in recycle boxes or totes, and
- colored paper, photos, and software manuals in the trash.

"NEVER recycle UCI and NEVER place it whole in the regular trash!"

DISPOSING OF COMPUTER HARDWARE

Before you transfer ownership or dispose of your computer, determine if any information needs to be retained or removed.

If the information needs to be retained:

transfer the information to another person who has proper authorization and need-to-know, by transferring to another computer, server or removable media.

If the information needs to be removed:

use a corporate-approved method, for either:

- clearing or,
- sanitizing.

"Transfer any information that needs to be retained, then remove the data before getting rid of a hard drive."

You cannot clear or sanitize your hard drive merely by using *delete, erase*, or *format* commands. In most cases, these commands only delete the file names from the directory, and leave the information on your system. To remove all files use an approved clearing method or sanitize by degaussing.

DISPOSING OF REMOVABLE ELECTRONIC MEDIA (REM)

"Removable Electronic Media" (REM) is a term used to describe disks, tapes, cartridges, jaz cartridges, CDs, zip drives and removable hard drives.

By disposing of removable electronic media correctly, you prevent unintended loss of Sandia information.

How you dispose of UCI and Unclassified REM depends upon your location.

- **At SNL/NM:** Use Removable Electronic Media Deposit Boxes; refer to the Computer Security Home Page for a list of locations.

  Removable media must be disposed of in these deposit boxes in one piece. *It is no longer necessary to cut, break, bend, or shred this media prior to disposal.*

  For large volume pick-up, contact the Hazardous and Solid Waste Department.

- **At SNL/CA:** Contact Property Coordinators for California guidelines and to make arrangements for pick-up.

- **At Remote Sites:** Follow remote site disposal procedures. *Remember nothing should go in the trash in one piece.*

"ONLY drop UNCLASSIFIED electronic media into Removable Electronic Media Deposit Boxes; NO paper and NO classified!"

Module 3: Practice Scenario

You need to answer the questions for this module before you continue.

Scenario
You have accepted a new position and have been authorized to purchase a new computer. The previous employee left different types of media and paper work that you do not need, as well as an old computer. Your new manager has advised you that you will be working on UCI project and you will need to have a modem connection to communicate with your offsite customer.

1. How will you ensure that the project information is recoverable?

   (A) Both B and C are appropriate ways to ensure your project information is recoverable.

   (B) You will back up your information to the department server, which is backed up weekly.

   (C) You will back up your information to the SDSS, which is backed up nightly.

   (D) You will save your information on your non-removable hard drive.

2. What action do you need to take before using the modem?

   (A) Call Telecon.

   (B) Read the Electrical Safety Manual.

   (C) Register the modem telephone line.

   (D) Both A and B are the actions to take before using a modem.

3. Before disposing of recorded information, what action do you need to take?

   (A) Check the Records Retention and Disposition Schedule.

   (B) Check Document Control Procedures Manual.

   (C) Contact your Computer Support Unit.

   (D) All the above are correct answers.

4. How will you dispose of Unclassified Controlled Information (UCI) paper and photos?

   (A) Shred prior to placing in the trash.

(B) Place in recycle box.

(C) Place in white burn bag (NM), or UCI mailbox (CA).

(D) Both A and C are correct ways to dispose of UCI.

5. How will you dispose of unclassified removable electronic media?

   (A) Place in an Removable Electronic Media Deposit Box (NM).

   (B) All of these are correct, depending upon your location.

   (C) Follow remote site procedures.

   (D) Contact Property Reapplication (CA).

6. What do you need to determine before you send the old computer to reapplication?

   (A) If any information needs to be transferred.

   (B) What information needs to be removed.

   (C) When the information needs to be encrypted.

   (D) Both A & B are correct.

Module 4
How to Protect UCI Information: What Additional Controls are Necessary?

At the end of this module, you will be able to identify additional guidelines for protecting Unclassified Controlled Information (UCI). These include guidelines for:

- authorization,
- additional controls,
- release/transmittal, and
- labeling/marking.

AUTHORIZATION

Using information appropriately means honoring any Need-to-Know (NTK) restrictions and managing the information as a Sandia asset.

Only users who are authorized and have a need-to-know may have access to Unclassified Controlled Information (UCI).

Your manager authorizes your need to process UCI information.

"UCI is sensitive; prior to processing, you must be authorized and have a need-to-know!"

ADDITIONAL CONTROLS FOR UCI

Your manager is responsible for determining what additional protection is required for Unclassified Controlled Information (UCI) owned by your Center.

Electronic UCI controls are documented in your Center Information Plan (CIP). This plan covers all locations, people, platforms, and unclassified information for which your Center is responsible. To obtain a copy of your CIP, contact your Computer Security Representative (CSR).

"You need to be familiar with the required controls in your Center Information Plan!"

You may be required to implement some or all of these types of controls.

For printed material:

- using Access Control Lists,
- restricting Foreign National access,
- special marking and covers, and/or
- storing in locked containers.

For information on electronic media:

- using Access Control Lists,
- restricting Foreign National access,
- prohibiting modem connections,
- prohibiting remote access,
- using encryption protection,
- applying additional passwords,
- activating audit logs, and/or
- storing on a protected server.

RELEASE/TRANSMITTAL OF UCI

Release of UCI

Releasing Unclassified Controlled Information (UCI) without permission or appropriate reviews causes a risk to Sandia.

Unclassified Controlled Information (UCI) should not be released without permission from the originator.

Prior to releasing Unclassified Controlled Information (UCI), you must follow the appropriate requirements and guidelines for getting your type of information and communication reviewed and approved.

Electronic Transmittal of UCI

Secure methods of electronically transmitting Unclassified Controlled Information (UCI) include:

- *secure* file transfer protocol (FTP),
- *secure* extranets,
- Web Fileshare *with access control*, and
- encryption.

"Encryption" is a term used to describe the process of scrambling information in a way so that only authorized users can unscramble it.

There are several UCI categories that MUST be encrypted when transmitted. Always check the Classification and Information Security Homepage for the current requirements.

Various hardware and software encryption methods are available for use at Sandia (e.g., Entrust, PGP).

"NEVER use the DropZone to transfer UCI files without protection; remember, the DropZone is open to anyone with access to the SRN!"

Sending UCI Printed Material

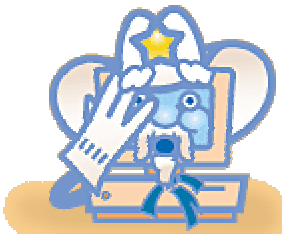
You may transmit UCI printed material by any of the following methods:

- internal mail,
- external mail, or
- facsimile (FAX).

Prior to sending, you need to provide appropriate security measures. The Unclassified Controlled Information CPR provides approved sending methods by UCI category.

In addition, your UCI documents may require supplemental access limitations (e.g., Specified Dissemination).

"Always provide appropriate protections prior to sending UCI!"



MARKING/LABELING UCI

You are responsible for marking and labeling your UCI appropriately.

Do NOT mark your information "UCI". Remember there are many categories of UCI. Use markings appropriate for the specific category of information.

When marking or labeling UCI . . .

For printed material:

- use UCI cover sheets or envelopes when appropriate; and
- mark according to the specific UCI category.

For electronic media:

- ensure that the UCI category is plainly visible;
- labels should only be one layer thick; and
- labels should not interfere with the drive mechanism.

"You MUST label by category all UCI documents and media (including backup copies) and store securely!"

Module 4: Practice Scenario

You need to answer the questions for this module before you continue.

Scenario
You have been assigned to an Unclassified Controlled Information (UCI) project. The project manager has requested that you distribute project data to team members using the DropZone, and daily back up the data to a disk.

1. Where would you find what protections are required for UCI in your Center?

   (A) None of these.

   (B) The Center Information Plan.

   (C) Your Computer Support Unit.

   (D) The Corporate Computing Help Desk.

2. Before distribution, what must you do?

   (A) Both B and D are correct.

   (B) Make sure all members of the group are authorized.

   (C) No action is needed before distribution.

   (D) Put it in a folder on the DropZone with protection.

3. What should you do with the back-up disk?

   (A) Give the disk to your manager without marking it.

   (B) Lock up the disk in your drawer without marking it.

   (C) Label the disk with UCI category, and store securely.

   (D) Leave the unmarked disk in your computer.

Module 5
How to Stay Out of Trouble: Cautions When Using Information Resources

After completing this module, you will be able to:

- use SNL information resources appropriately,
- avoid waste, fraud, and abuse,
- recognize transmission security (Red/Black) issues,
- recognize and report a security incident involving information resources,
- use Personal Electronic Devices (PEDs) appropriately,
- explain the conditions for installing and copying software at SNL, and
- apply the rules for using software available from public sources.

APPROPRIATE USE OF INFORMATION RESOURCES

Rules about the use of information resources (internet/intranet connections, computers, printers, copiers, and telecommunications services/capabilities) apply to:

- all employees, contractors, and visitors,
- all locations including on-site, off-site, and home, and
- all computers (laptop to mainframe).

"Ask yourself if you'd feel comfortable obtaining the same information some other way, and defending your use with your manager. If the answer is yes, then it's o.k. to use the Internet!"

All information resources are to be used exclusively for work-related purposes or approved incidental personal use.

Use the following criteria for determining appropriate incidental personal use:

- clear benefit to Sandia,
- insignificant cost, and
- efficient/effective use of your time.

For additional criteria, see CPR 400.2.13.5 referenced in the Straight Shot.

CAUTIONS WHEN USING SNL COMPUTER RESOURCES

"Don't go where you don't belong — another desktop, server or network — without authorization!"

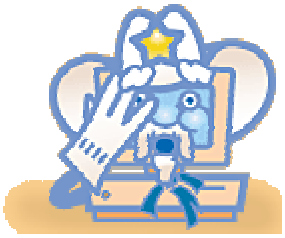
People don't have to touch your computer to access your information — they can connect to your computer through networks.

Don't have any expectations for privacy.

Everything is subject to monitoring including:

- computer files,
- computer configurations,
- electronic e-mail, and
- Internet /intranet access (24/7).

"Realize that anything you do on your computer can be seen; don't write anything that you don't want someone else to read."



Computing From Home or Remote Locations

Telecommuting

If you elect to telecommute as a Sandia employee, it is your responsibility to be familiar with the SNL telecommuting policy.

When telecommuting, you:

- may only process Unclassified information, and

- must adhere to all Sandia guidelines for processing, managing, and protecting information.

Remote Access

When computing from home or from any other non-Sandia location, you need to apply the same guidelines as noted in the Telecommuting CPR.

WASTE, FRAUD, AND ABUSE

Waste, Fraud, and Abuse of information resources are incidents and must be reported. Penalties for misuse of SNL resources range from disciplinary action to prosecution by the Office of the Inspector General.

"Waste, Fraud and Abuse (WFA) will not be tolerated."

Waste

Don't waste information resources at Sandia by:

- purchasing equipment or software that is not needed,
- purchasing more products than are needed, or
- purchasing products with more capability than required.

Fraud

Don't defraud Sandia by:

- purchasing equipment or software for personal use, or
- stealing Government resources (e.g. office supplies, books, CDs, etc.)

Abuse

Don't abuse information resources by:

- improper access or use that causes information loss, or
- improper handling or neglect that causes equipment damage.

"Don't let your data be compromised by loss, damage, or unauthorized access.

You're entrusted with Government resources, and you must provide the care necessary to maintain its useful life."

TRANSMISSION SECURITY - RED/BLACK SEPARATION

At Sandia, several problems were discovered during a recent survey of telecommunications security. Members of the workforce were not aware of the risks associated with having classified and unclassified in the same building, work area or cubicle.

Equipment and signal wiring used for processing classified (RED) information must maintain prescribed separation from equipment and cables processing unclassified (BLACK) information.

If you need classified and unclassified in the same area (building, work space or cubicle), you need to separate Red and Black according to distances specified in the Transmission Security Checklist.

Separation distances must extend into spaces beyond walls, ceilings, and floors.

Violation of Red/Black separation could cause the loss of classified information, resulting in a security incident.

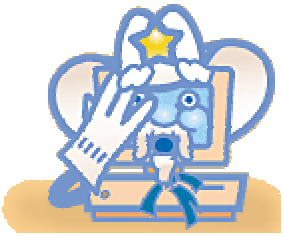
"Remember, if there is classified around anywhere separate RED and BLACK!"

SECURITY INCIDENTS INVOLVING INFORMATION RESOURCES

A security incident involving information resources is caused by:

- failure to comply with security regulations/directives,
- waste, fraud, and abuse of resources, or
- attempted, suspected, or actual compromise of information.

All members of the workforce are responsible for reporting security concerns.



"If you suspect an incident, call the incident pager immediately."

How To Report A Security Incident

Immediately call the Security Incident Management Program (SIMP) pager:

- 540-2580 (SNL/NM and SNL remote sites), or
- 294-3238 (SNL/CA).

Do not discuss details of the incident via telephone, alphanumeric pager, e-mail, or voice-mail.

An inquiry official will contact you.

CAUTIONS WHEN USING PERSONAL ELECTRONIC DEVICES (PEDs)

PED Areas of Concern

The following are areas of concern when using PEDs:

- microphones (recording and transmitting capabilities),
- unauthorized downloading and uploading (data exchange capabilities), and
- unauthorized software code exploitation.

"You MUST consult the Prohibited and Controlled Items CPR before purchasing a PED!"

PED Guidelines

Before a contractor or visitor can bring in a company-owned PED to an SNL site, the Request for Contractor/Visitor Computers must be completed and approved.

Typically, no personally owned PEDs are allowed in the Property Protection Areas or Limited Areas.

Before you purchase, know the capabilities of the PED.

After you purchase a PED, know how to manage its capabilities.

Always turn your PED off when not in use.

CAUTIONS WHEN INSTALLING AND COPYING SOFTWARE

Software license agreements accompany most software. These agreements between the vendor and SNL explain the conditions for installing and copying the software.

"SNL does not permit the violation of software licenses or copyright laws, even for a limited time period."

Unless software is site-licensed by SNL, users are required to have one of the following to verify their right to have a software product on their system:

- vendor license agreement,
- purchase order or proof of payment,
- original documentation, or
- original disks.

"All software needs to be scanned for viruses before installation."

CAUTIONS WHEN USING SOFTWARE FROM PUBLIC SOURCES

Shareware/freeware and public domain software are terms to describe software available from public sources.

Because this type of software could easily contain hidden code or viruses, SNL discourages you from using this software on SNL computer systems. You must not install software that could impact the SNL network infrastructure, unless tested prior to use.

Software created by or for Sandia is not considered public source software.

Guidelines for using software from public sources:

- It must meet a specific business need.
- No comparable software is available from Sandia resources.
- It must be tested for viruses.
- You must follow the copyright license.
- You must be able to show proof of payment (if required by license agreement).

"Be aware that public source software may contain hidden features that could cause damage to your computer, your files, and SNL's networks."

Module 5: Practice Scenario

You need to answer the questions for this module before you continue.

Scenario
You have a desktop connection to the Sandia Restricted Network and a laptop. You plan to purchase a Personal Electronic Device. You also have a personal home computer. You work on site, on travel and at home.

1. You need to do extensive research on vacation sites on the Internet. Which computer can you use?

   (A) SNL desktop at work.

   (B) SNL laptop at home.

   (C) Personal home computer.

   (D) Any of the above.

2. What do you need to do before installing new software on your SNL desktop?

   (A) Read the software license agreement.

   (B) Read the software user manual.

   (C) Scan the software disk for virus.

   (D) Both A & C are correct.

3. Before you purchase a Personal Electronic Device (PED), what do you need to know?

   (A) Both B and C are correct.

   (B) What PED features are allowed.

   (C) The common areas of concern.

   (D) The GPO specifications.

4. You are reading an e-mail on your SNL computer and suspect that the information is classified. Whom do you contact immediately?

   (A) Reply to sender.

   (B) Call the SIMP pager.

(C) No one, just delete.

(D) Forward to your CSR.

5. When using public source software, what guidelines do you need to be aware of?

   (A) The software meets a business need and is virus checked.

   (B) All public source software has been virus checked.

   (C) There is never a payment for public source software.

   (D) There is always commercial software available.

6. You are rearranging your workspace. The workspace next to you contains classified equipment. What do you need to consider?

   (A) Red/Yellow connections.

   (B) A and C are both correct.

   (C) Red/Black separation.

   (D) None of these.

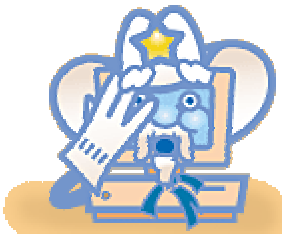
Module 6
How to Minimize Risk: Beware of Theives and Outlaws!

After completing this module, you will be able to minimize the risk of your information being tampered with, lost, or stolen:

- by insiders penetrating your computer's information,
- by outsiders penetrating your computer's information, and
- when traveling with Sandia information.

RISK OF INSIDER THREAT

"Beware! Insider threat does exist."



Every person at Sandia must have a basic understanding of the vulnerabilities inherent within his or her work area.

Disgruntled or dishonest employees pose a high threat to corporations; it is estimated that insiders with grudges are responsible for over 70% of successful attacks on information systems.

How It Happens

Sticky Fingers — The most obvious way to steal information is to snatch it from unprotected files.

Dumpster Diving — Thieves often comb the trash (including wastebaskets) for useful documents that weren't properly destroyed.

Shoulder Surfing — Information may be obtained illicitly simply by someone standing close enough to look over your shoulder.

Inside Job — Insiders usually know what precautions are in place, and they may have the ability to exploit weaknesses found in computer applications, systems, networks and business practices used in managing information.

"Ask yourself, "Have I provided sufficient protection for Sandia information?"

Be sure that appropriate protective measures are in place. Should your computer or information be accessed, make sure that the loss of the information would not place you or Sandia National Laboratories in a vulnerable position.

"Ask yourself, "Would information found in my files place me or Sandia in jeopardy?"

How To Minimize Risk From Insider Threat

Always be aware of the potential for insider threats. You are responsible for protecting Sandia's information from unauthorized reading, editing and copying.

Pay attention to unusual people and occurrences.

Be alert to the following possible indicators of insider threat:

- alteration of documents,
- improperly badged personnel,
- an unknown individual in your work area,
- unauthorized access to your files, or
- changed passwords.

"Protect SNL Information from sticky fingers and dumpster thieves by disposing of paper and media correctly!"

RISK OF OUTSIDER THREAT

Risk of Attack from Outside Sandia

New technologies are creating new opportunities for hackers. Our networks are constantly under attack, and the attacks are increasing. Attackers are global, and acquiring new skills daily.

Consequences of a Successful Attack

The following are potential negative consequences of a successful attack from someone outside Sandia:

- information loss,
- changed source code,
- damaged reputation as the primary national security laboratory,
- public lack of confidence in the security of our national laboratories,
- liability if a Sandia system is penetrated, taken over, and used to attack other systems, and
- liability if Sandia servers are used to distribute illegal copies of software.

"Don't put copyrighted material on the drop zone for distribution unless it's site licensed!"

How To Minimize Risk of Attack from Outside Sandia

There are many things you can do to reduce the chances of your computer being compromised. Practice "safe computing" by:

- following the minimum desktop protection guidelines,
- protecting your password,
- registering your computer system(s) in NWIS,
- applying computer software "patches" (fixes) when requested by computer security representatives, and
- not changing your system's configuration once it's set up. Computer Support Unit technicians and system administrators set up Sandia computers to meet computer security configuration guidelines.

RISK WHEN TRAVELING WITH SANDIA INFORMATION

When on travel you must "maintain control" of handcarried equipment, information, and technology at all times. Leaving your portable computer or UCI documents unattended puts Sandia at risk.

How To Minimize Risk When Traveling

Never leave your information unattended in:

- a hotel room/baggage check,
- the trunk of a car/valet parking, or
- an exhibit hall/demo room.

"When traveling, never leave your computer or UCI documents unattended!"

Your information could be:

- infected with viruses, codes, or worms,
- examined and have data removed (unauthorized access),
- confiscated by unauthorized personnel, or
- stolen or copied.

International Travel Requires Additional Precautions

Before Leaving
When preparing to travel to a foreign country, visit the International Handcarry section of the Export & Import Controls Homepage.

After Returning
When you return from travel to a **sensitive** foreign country have your portable computer inspected by the Electronic Security Systems Department, Technical Surveillance and Countermeasures (TSCM).

"No matter where you travel, make sure you safeguard your UCI files."

Module 6: Practice Scenarios

You need to answer the questions for this module before you continue.

Scenario 1
You are working on a UCI document, which is kept on your department's local server. You are located in the Limited Area.

1. How can you minimize the risk of your information being tampered with by **insiders**?

   (A) Pay attention to changed passwords.

   (B) Both a and c are correct.

   (C) Be alert to unauthorized access to your files.

   (D) There is no reason for concern because all people are badged.

2. How can you minimize the risk of your information being tampered with by **outsiders**?

   (A) Change your system's configuration.

   (B) Follow the Minimum Desktop Protection guidelines.

   (C) Apply computer software "patches" when requested.

   (D) Both b and c are correct.

Scenario 2
You are traveling to China to investigate the possibility of a new "Work for Others" project. You will be bringing along your portable computer for your "slide-show" presentation. While on travel, you also plan to work on several documents from other projects and access your e-mail on the portable computer. After your presentation, your hosts have invited you to lunch.

1. What action(s) do you need to take BEFORE you travel?

   (A) Visit the Export & Import Controls Homepage.

   (B) Visit the Recorded Information Management Homepage.

   (C) Visit the Technical Surveillance and Countermeasures Homepage.

   (D) You need to do all of the above.

2. What action(s) do you need to take while you are at lunch?

(A) You leave your portable computer in the trunk of a vehicle.

(B) You leave your portable computer in the demo room.

(C) You check your portable computer with your luggage.

(D) You take your portable computer with you.

3. What action(s) do you need to take AFTER you return from your travel?

(A) You have your portable computer inspected by CCHD.

(B) You have your portable computer inspected by your CSU.

(C) You have your portable computer inspected by TSCM.

(D) You have your portable computer inspected by your CSR.